Math 557 Nov 7

Practice on PA and Computability

The power of induction

Recall the axioms of PA:

- **P1** $Sx \neq 0$
- **P2** $Sx = Sy \to x = y$
- **P3** $x + 0 = x$
- **P4** $x + Sy = S(x + y)$
- **P5** $x \cdot 0 = 0$
- **P6** $x \cdot Sy = x \cdot y + x$
- $\mathbf{Ind}_\varphi$ $\varphi(0) \land \forall x(\varphi(x) \to \varphi(Sx)) \to \forall x\, \varphi(x)$

Exercise 0.1.
Show that $\mathsf{PA} \vdash \forall x(Sx \neq x)$

But we need induction to prove this, even if we throw in another axiom:

- **P7** $\forall x\, (x \neq 0 \to \exists y(x = Sy))$

The system (P1)-(P7) is referred to as **Robinson's Q**

Exercise 0.2.
Show that $Q \nvdash \forall x(Sx \neq x)$

(*Construct a model of Q by adding a "point at infinity" to $\mathbb{N}$ and defining the operations $S, +$ accordingly.*)

If we use induction in the *metatheory* (i.e. the theory we are using to reason about Q, PA, etc.), we can still show

$$\text{for all } n \in \mathbb{N}, \quad \mathsf{Q} \vdash S\underline{n} \neq \underline{n}$$

Capturing basic arithmetic of $\mathbb{N}$ in PA^-

We saw in class that PA^- proves all true Σ_1-statements about $\mathbb{N}$. This is due to two facts:

- Δ_0-formulas are **absolute between structures and end-extensions thereof**.
- Any model $\mathcal{M}$ of PA^- is an end-extension of (an isomorphic copy of) $\mathbb{N}$.

To prove the second fact, we need to show two things:

1. The mapping $\iota : n \mapsto \underline{n}^{\mathcal{M}}$ is an embedding (so $\iota(\mathbb{N})$ is a substructure of $\mathcal{M}$ isomorphic to $\mathbb{N}$).
2. Any element $y \in M$ with $y <^{\mathcal{M}} \underline{n}^{\mathcal{M}}$ is itself some $\underline{m}^{\mathcal{M}}$.

The first item is established in the next exercise.

Exercise 0.3.
Show that for all natural numbers n, k, l,

$$\begin{aligned} n = k + l \quad &\Longrightarrow \quad \mathsf{PA}^- \vdash \underline{n} = \underline{k} + \underline{l} \\ n = k \cdot l \quad &\Longrightarrow \quad \mathsf{PA}^- \vdash \underline{n} = \underline{k} \cdot \underline{l} \\ n < k \quad &\Longrightarrow \quad \mathsf{PA}^- \vdash \underline{n} < \underline{k} \end{aligned}$$

(*You prove this by induction in the metatheory. For example, for the first statement, the case $k = 0$ follows from axiom (A6). For the inductive step, use axiom (A1).*)

For the second item:

Exercise 0.4.
Show that for all $k \in \mathbb{N}$,

$$\mathsf{PA}^- \vdash \forall x\, (x \leq \underline{k} \rightarrow (x = \underline{0} \ \vee \dots \vee \ x = \underline{k})$$

Again, use (meta-) induction on k. The case $k = 0$ follows from (A15). For the inductive step, show

$$\mathsf{PA}^- \vdash \forall x, y\, (y > x \rightarrow y \geq x + 1)$$

More on the limitations of PA^-

Exercise 0.5.
Let R be the ring $\mathbb{Z}[X, Y]/(X^2 - 2Y^2)$, i.e., R is the polynomial ring $mathbbZ[X, Y]$ modulo the equivalence

$$p(X, Y) \sim q(X, Y) \quad :\Longleftrightarrow \quad p - q = r(X^2 - 2Y^2).$$

Show that R can be discretely ordered.

Infer that

$$\mathsf{PA}^- \nvdash \forall x, y\, (x > 1 \rightarrow x^2 \neq 2y^2)$$

Number theoretic functions

Exercise 0.6.
Show that the following relations and functions are primitive recursive.

$$\begin{aligned}
&x \text{ divides } y \\
&\mathrm{rem}(x, y) \text{ (remainder when } y \text{ is divided by } x) \\
&x \text{ is prime} \\
&n \mapsto p_n, \text{ where } p_n \text{ is the } n\text{th prime}
\end{aligned}$$

Gödel's Lemma

If you feel like it, try your hands at proving Gödel's famous Lemma on the β function:

Lemma 0.1 (Gödel's Lemma)**.**
There exists a primitive recursive function β such that for every k and for every finite sequence $x_0, x_1, \dots x_{k-1} \in \mathbb{N}$, there exists a natural number c with

$$\textit{for all } i < k: \ \beta(c, i) = x_i.$$

In fact, there exists a Δ_0-formula $\theta(x, y, z)$ such that

$$\mathbb{N} \models \forall x, y\, \exists! z\, \theta(x, y, z),$$

and the formula $\theta(x, y, z)$ defines the function β over the natural numbers.

Hint: To code a sequence $x_0, x_1, \dots x_{k-1}$ of natural numbers, set $m = b!$ where $b = \max(k, x_0, x_1, \dots x_{k-1})$. Verify the numbers

$$m + 1, 2m + 1, \dots k \cdot m + 1$$

are pairwise coprime. Now try to apply the *Chinese Remainder Theorem*.